COMMONWEALTH of VIRGINIA

DEPARTMENT OF MEDICAL ASSISTANCE SERVICES
600 East Broad Street, Suite 1300
Richmond, VA 23219

May 11, 2007

ADDENDUM No. 1 TO VENDORS:

Reference Request for Proposal:	**RFP 2007-06**
Dated:	**April 30, 2007**
Due:	**June 4, 2007**

Item 1 - Change

On Page 3 - "**General Scope of Responsibilities**: The successful contractor will conduct an accurate and thorough business impact analysis/assessment (BIA) of all fourteen DMAS Divisions and a Risk Analysis (RA) of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by DMAS, prepare a risk management plan and also conduct an assessment of the staffing needs of the Office of Compliance and Security."

Is changed/amended to read:

General Scope of Responsibilities: The successful contractor will conduct an accurate and thorough business impact analysis/assessment (BIA) and a Risk Analysis (RA) of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all information held by DMAS, and prepare a Risk Management plan. This BIA/RA will encompass all administrative and operational Divisions at 600 East Broad Street.

****

Item 2 – Change

On Page 4 - **"3.1. Review of DMAS's Current Security Posture**

At the direction of the DMAS Compliance and Security Officer the selected vendor will conduct an accurate and thorough business impact analysis/assessment (BIA) of all fourteen DMAS Divisions and a Risk Analysis (RA) of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by DMAS, prepare a risk management plan and also conduct an assessment of the staffing needs of the Office of Compliance and Security."

Is changed/amended to read:

3.1. Review of DMAS's Current Security Posture

At the direction of the DMAS Compliance and Security Officer the successful contractor will conduct an accurate and thorough business impact analysis/assessment (BIA) and a Risk Analysis (RA) of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all information held by DMAS, and prepare a Risk Management plan. This BIA/RA will encompass all administrative and operational Divisions at 600 East Broad Street.

****

Item 3 – Delete

On page 4 – "**3.2** Preparation of the OCS Staffing Plan

The vendor will be required to assist the DMAS Compliance and Security Officer in the preparation of a staffing plan for the DMAS OCS. "

3.2 Preparation of the OCS Staffing Plan - Is Deleted**.**

****

Item 4 – Change

"3.3. OCS Risk Management Plan

As a deliverable to the work performed under this contract the vendor will prepare a risk management plan. This document will recommend and detail all activities and projects to be carried out during the next two years."

Is changed/amended to read

3.3. OCS Risk Management Plan

As a deliverable to the work performed under this contract the vendor will prepare a Risk Management plan.

****

Item 5 - Change

On page 11 - **"5.1.15 Chapter Five: Project Work Plan**

The proposal shall describe the following:

Work Plan and Project Management: The proposal shall include a work plan (Microsoft Word format) detailing the sequence of events and the time required to complete this project no later than sixty days after contract execution or as negotiated during the RFP process. The relationship between key staff and the specific tasks and assignments proposed to accomplish the scope of work shall also be included. A PERT, Gantt, or Bar Chart that clearly outlines the project timetable from beginning to end shall be included in the proposal. Key dates and key

events relative to the project shall be clearly described on the chart including critical path of tasks. The Offeror shall describe its management approach and how its proposed work plan will be executed.

Progress Reports: Upon award of a contract, the Contractor must prepare a written progress report, as well as telephonic meetings, every week or more frequently as necessary and present this report to the DMAS Compliance and Security Officer or his designee. The report must include:

1. Status of major activities and tasks in relation to the Contractor's work plan, including specific tasks completed for each part of the project.
2. Target dates for completion of remaining or upcoming tasks/activities.
3. Any potential delays or problems anticipated or encountered in reaching target dates and the reason for such delays.
4. Any revisions to the overall work schedule."

Is changed/amended to read

5.1.15 Chapter Five: Project Work Plan

The proposal shall describe the following:

Work Plan and Project Management: The proposal shall include a work plan (Microsoft Word format) detailing the sequence of events and the time required to complete this project. *The Department anticipates this project could be completed within sixty days after contract execution. However, based upon the work plan submitted with the RFP response, this sixty day time frame may be negotiable during the RFP evaluation process*. (Emphasis added).

- The relationship between key staff and the specific tasks and assignments proposed to accomplish the scope of work shall also be included.
- A PERT, Gantt, or Bar Chart that clearly outlines the project timetable from beginning to end shall also be included in the proposal.
- Key dates and key events relative to the project shall be clearly described on the chart including critical path of tasks.
- The Offeror shall describe its management approach and how its proposed work plan will be executed.

Progress Reports: Upon award of a contract, the Contractor must submit a weekly project status report (via e-mail in an attachment in MS Word format) to the DMAS Compliance and Security Officer or his designee. At a minimum, the report must include:

1. Status of major activities and tasks in relation to the Contractor's work plan, including specific tasks completed for each part of the project.
2. Target dates for completion of remaining or upcoming tasks/activities.
3. Any potential delays or problems anticipated or encountered in reaching target dates and the reason for such delays.
4. Any revisions to the overall work schedule.

****

Item 6 - Delete

Section 6.2.2, third bullet, delete the last sentence

****

Item 7 - Replace

Attachments C, Cost Proposal, delete the current attachment and replace with Revised Cost Proposal Format.

****

Item 8 - New Term and Condition:

Addition of section 10.24: ADDITIONAL USERS: Any agency within the Health and Human Resources Secretariat (HHR) may purchase Risk Assessment, Business Impact Analysis, Risk Mitigations Planning or other security-related consulting services from this contract at the negotiated hourly rates. The winning offeror may not market their services to the HHR agencies. DMAS (OCS) will remain the point of contact for notifying agencies of the HHR of this contract and for coordinating any related purchase orders.

****

Item 9 – Change;

Due date for receipt of proposals is changed to June 4, 2007, 2:00 PM local time.

****

See attached questions and responses related to the referenced RFP.

Note: A signed acknowledgment of this addendum must be received by this office either prior to the due date and hour required or attached to your proposal response. Signature on this addendum does not substitute for your signature on the original proposal document. The original proposal document must be signed.

Sincerely,

William D. Sydnor

William D. Sydnor
Contract Management Director

Name of Firm: _____

Signature and Title: _____

Date: _____

1.	What is the relationship between the IM division and OCS regarding computer security, and how do their responsibilities differ?	The *Office of Compliance and Security (OCS)* is responsible for security governance and oversight (e.g., Chair the DMAS Security Advisory Committee (SAC), develop security policies and awareness training, manage DMAS Continuity of Operations (COOP), review of overall security operations, HIPAA Compliance and Risk Management in compliance with the VITA's Information Technology Risk Management Guidelines SEC 506-01 dated 12/11/06 and the HIPAA Security Rule standard of §164.308(a)(1)(ii)(B).), The *Information Management (IM) Division* is responsible for security implementation (e.g., technical security implementation, Active Directory account maintenance, firewalls, HelpDesk, configuration and operations management, incident response, IT Disaster Recovery and Contingency plans, management of DMAS data center and servers, management of the VaMMIS system, etc.).
2.	What, if any, information security staffs do the OCS and the IM divisions presently have?	See Q1
3.	To what extent would the OCS and IM staff be available to assist and support in the risk assessment and subsequent risk management activities?	OCS will manage the contract. IM will be available for interviews during the BIA/RA processes.
4.	Has a technical vulnerability test been performed within the past 6 months? 12 months?	Yes
5.	Is IM responsible for all software applications used by DMAS, including both purchased and developed? If not, please explain.	Yes
6.	Approximately how many applications does IM support? Approximately how many of those applications or systems contain patient/subscriber-identifiable health data?	This information will be discussed with offerors selected for negotiations. DMAS expects the results of the BIA and RA will clarify and verify how many applications or systems contain patient/subscriber-identifiable health data.

7.	What network operating systems (NOS) and operating systems (OS) are supported?	This information will be discussed with offerors selected for negotiations.
8.	What Data Base Management Systems (DBMSs) are supported?	This information will be discussed with offerors selected for negotiations.
9.	Does DMAS have a wireless LAN or other wireless capability?	Yes.
10.	Will VITA [*Virginia Information Technologies Agency*] have any involvement in this RFP process? Will VITA be reviewing or signing off on the Vendor's plans and work?	No.
11.	Generally, to what extent is DMAS in compliance with the VITA security policy and standard? Has DMAS been compliant with previous VITA security requirements?	DMAS is required to comply with VITA Security Policy and Standard, published in July 2006.
12.	Are there any government caps that could affect the contract, such as a cap on hourly rate? on the overall contract amount? on expenses? Are there any particular government restrictions other than as noted in the RFP?	Refer to **6.2.4 Cost** (Attachment C) **20%** The cost proposal shall be evaluated and weighted but is not the sole deciding factor for the RFP.
13.	Is privacy – e.g., HIPAA privacy rule compliance – intended to be included in the scope of this contract? If so, is it limited to HIPAA privacy rule considerations? If privacy is included in the scope, is the OCS Privacy Office currently staffed?	Yes. No Yes

14.	The RFP section 3. Scope of Services states that the risk assessment cover risks to electronic protected health information. Does the OCS intend that the assessment also cover other forms of such information as protected by HIPAA's privacy rule?	Refer to Item 2 in the Addendum.
15.	The RFP sections 1 and 3 call for a "business impact analysis/assessment (BIA) … and a Risk Analysis (RA)." Since those terms can have different connotations for different individuals, please expand and clarify what OCS intends by those terms in the context of this RFP.	As required in 5.1.11 in item 1, Understanding of the project requirements, offerors should provide evidence of their understanding of the terms BIA and RA, as they relate this project. For additional information refer to the references provided on page 4 of the RFP: VITA http://www.vita.virginia.gov/docs/psg.cfm VDEM http://www.vaemergency.com/library/coop/resources/index.cfm HIPAA Privacy and Security Rules at http://www.cms.hhs.gov
16.	Under RFP section 5. Proposal Preparation and Submission Requirements, section 5.1.15 describes the Project Work Plan: "The proposal shall include a work plan … detailing the sequence of events and the time required to complete this project no later than sixty days after contract execution or as negotiated during the RFP process." Please clarify.	Refer to Addendum, Item 5

17.	Since the RFP states, "The proposal shall include a work plan," it is unclear what is subsequently due "no later than sixty days from contract execution." A reliable work plan submitted at the time of the proposal can only be a very high-level plan that would not appear to meet the RFP's requirement for specific details. Is it the intent of the RFP for Vendors to submit a high-level plan with the proposal, and a more detailed work plan at a later date?	Refer to Addendum, Item 5
18.	Does the OCS have a timeframe in mind for completion of the review and assessment (RFP section 3.1)? RFP page 4, item 3.3 implies that a risk management plan would be completed in year 1 so that the "activities and projects" detailed in the plan would be carried out in years 2 and 3. Is that statement a guideline, or is it a requirement?	Refer to Addendum, Item 4 & Item 5
19.	How would the OCS compare the importance of cost versus speed?	OCS will not compare price versus speed.
20.	Does the OCS have an anticipated date for a decision on this RFP?	Once the evaluation process is completed a decision on the award for this RFP will be made.

21.	Page 3, Section 1 and Page 4, Section 3: The RFP states the contract is for three years with up to two additional one-year renewals. Are the tasks outlined in Section 3 (Scope of Services) one-time events or will these be updated by the selected Consultant on an annual basis? If the former, can you explain what the contractor's responsibilities will be in years two and three (and beyond) of the contract?	Refer to Addendum, Item 5. Work in future years is not guaranteed; however, the winning vendor may be invited back in future years to perform additional compliance and security-related consulting work.
22.	Page 11, Section 5.1.15: The RFP states that "The proposal shall include a work plan (Microsoft Word format) detailing the sequence of events and the time required to complete this project no later than sixty days after contract execution…" Please clarify – is the work plan due within 60 days or is DMAS requesting that the full project scope be completed within 60 days? Is there a state deadline that must be met for the risk management and compliance plans?	Refer to Addendum, Item 5.
23.	Page 13, Section 6.2.3: Does DMAS require a specific percentage of small business entity involvement in the contracts it awards? If yes, what is that percentage?	No.
24.	When does DMAS expect to award this contract? Has the DMAS identified a preferred project start date and project completion date?	Once the evaluation process is completed a decision on the award for this RFP will be made. Refer to Addendum, Item 5.

25.	Are the DMAS's core systems (that maintain Medicaid, FAMIS, and PACE data) housed and maintained at DMAS, Virginia Information Technologies Agency (VITA), or other third party service center?	This information will be discussed with offerors selected for negotiations.
26.	How many computer staff and programmers are dedicated to supporting DMAS systems?	This information will be discussed with offerors selected for negotiations.
27.	How many staff are in the OCS? Can you briefly describe the organization structure and skill sets currently in place? Does the staff currently conduct security and compliance "audits" for DMAS?	This information will be discussed with offerors selected for negotiations.
28.	Does DMAS have risk management and compliance plans in place that can be updated or do these plans have to be prepared as part of this contract?	Preparation of a Risk Management Plan is a requirement of the RFP.
29.	Does DMAS have continuity plans in place that can be updated or do these plans have to be prepared as part of this contract?	Updating continuity plans is not within the scope of this RFP. This information may be discussed with offerors selected for negotiations.
30.	Is the government asking for system(s) vulnerability testing and analysis, or for a non-technical assessment of current vulnerabilities only?	Refer to Addendum Item I and Item 2
31.	What are the sizes and locations of the 14 divisions mentioned in the RFP?	This information will be discussed with offerors selected for negotiations.
32.	How many workstations are included in the vulnerability assessment?	This information will be discussed with offerors selected for negotiations.
33.	How many operating systems are there, and what are they?	This information will be discussed with offerors selected for negotiations.

34.	Does the government want scans or penetration testing (or both)?	Neither
35.	Will the contractor have access to security plans for the systems?	This information will be discussed with offerors selected for negotiations.
36.	Will the contractor have access to previous vulnerability assessments?	This information will be discussed with offerors selected for negotiations.
37.	Will the ISSO [*Information System Security Officer*] and System Administrator(s) be available during testing?	Refer to response to Q. 34
38.	Can a list of vendors the contractor will be required to work with be made available in order to asses any possible conflict of interest?	Offerors must be able to work with all members of DMAS workforce, including contractors. If an offerors have a conflict of interest with any particular contractor, they must identify that in their response to the RFP.
39.	Is the work to be performed on-site, off-site, or a combination of both?	Both
40.	Will there be travel involved, and if so will the government reimburse travel at the standard state authorized rates?	There is no travel involved in the fulfillment of requirements of this RFP.
41.	Is there a preferred vendor?	No
42.	Is there an incumbent vendor?	No
43.	Does the scope of the Risk Analysis requested in the RFP include only "Risk Analysis (RA) of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by DMAS" (Section 3.1), or does the scope of the Risk Analysis include potential risks and vulnerabilities to the confidentiality, integrity, and availability of all IT systems and data that DMAS classifies as sensitive, as required by SEC501-01?	As required in RFP 5.1.11 in item 1, Understanding of the project requirements, offerors should provide evidence of their understanding of the term RA, as it relates to this project. For additional information refer to the references provided on page 4 of the RFP: VITA http://www.vita.virginia.gov/docs/psg.cfm VDEM http://www.vaemergency.com/library/coop/resources/index.cfm HIPAA Privacy and Security Rules at http://www.cms.hhs.gov

44.	In conducting the Risk Analysis, does DMAS have a preference for: A single Risk Assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by DMAS (and other sensitive IT systems and data, if within scope); or Multiple Risk Assessments, organized by IT system, as envisioned by SEC501-01; Or is each Offeror free to propose its own approach?	See Q 43 Offerors are free to propose own approaches.
45.	To what extent has DMAS developed an inventory of IT systems, defined these IT systems, and classified these IT systems and the data they process according to sensitivity, and to what extent is this inventory, definition, and classification within the scope of the RFP.	This information will be discussed with offerors selected for negotiations.

46.	In order to assist Offerors in responding to the RFP, can DFS provide Offerors with any additional information regarding the nature and extent of its IT environment? Useful information would include Number of Sensitive, Non-sensitive; and HIPAA-related IT systems, and number and nature of components (servers, software, workstations, SANS, network infrastructure) associated with each. Distinct types of electronic protected health information and other sensitive electronic data (if within scope) held by DMAS. Number, types, and components of: Enterprise or centrally-managed; Divisionally-managed; and Single user IT systems that are within the scope of the RFP. Number and location of any DMAS or DMAS partner offices that are within the scope of the RFP.	This information will be discussed with offerors selected for negotiations.
47.	To what extent does the scope of the RFP include physical security?	See Q 43
48.	Is assessment of the compliance of DMAS' business partners with HIPAA and SEC501-01 within the scope of the RFP?	No
49.	May Offerors assume that the statement in section 3.3 "and <u>detail all</u> activities and projects to be carried out during the next two years" refers only to Risk Management activities?	Refer to Addendum Item 4

50.	Is conducting the projects and activities identified by the Offeror in the OCS Risk Management Plan within the scope of the RFP?	No
51.	Can DMAS provide Offerors with any additional insight regarding the requirement that "at least one staff member who is an Associate in the Society of Actuaries and a member of the American Academy of Actuaries"? What role in the project does DMAS envision for this individual?	As stated in the pre-proposal conference April 30, this bullet should be deleted.
52.	Does DMAS require that Offerors use VDEM COOP methodology for conducting the BIA, or may Offerors substitute their own methodology?	No, offerors substitute their own methodology.
53.	Is developing or updating a DMAS COOP or BCP within the scope of the RFP? If so, is the COOP or BCP limited to IT resources or enterprise-wide in scope?	No
54.	What circumstances drive the DMAS assumption that the project should last at least three and could last as long as five years? Does DMAS envision a constant level of effort by the successful Offeror throughout the three or five years?	See Q 21
55.	Based on answer to question above and our assumption that initial BIA/RA will not take three years, can DMAS provide guidance on how to price work for remainder of contract?	See Q 21

56.	What is DMAS requesting by the statement in section 5.1.15 - "The proposal shall include a work plan (Microsoft Word format) detailing the sequence of events and the time required to complete this project no later than sixty days after contract execution or as negotiated during the RFP process"? Is DMAS requesting that each Offerors proposal contain a work plan that describes its plan for developing a comprehensive task plan for the entire project within 60 days after contract execution?	Refer to Addendum, Item 5.
57.	To what extent does DMAS expect the offeror to provide its own methodologies or work under the guidance of the Office of Compliance and Security?	OCS manages contract. Offerors to propose their own methodology.
58.	Regarding the third deliverable, staffing plan, can you tell us how many employees are within the scope of this study?	Refer to Addendum, Item 1, Item 2 and Item 3.
59.	Please clarify the scope of the first year's work.	Refer to Addendum, Item 5.

60.	Questions regarding the meaning of "key staff" were asked and discussed.	"Key staff" means all individuals assigned to work on the project, in whatever capacity. Each key staff member must be identified to DMAS and will be required to sign appropriate confidentiality agreements. Also, all key staff members identified to DMAS will be listed (identified) in the Business Associate Agreement (BAA) required as part of the award of this contract. For information on BAAs, refer to the DMAS website at http://www.dmas.virginia.gov/hpa-home.htm.
61.	Questions regarding (1) DMAS data, information and PHI, (2) the use of vendor equipment or DMAS equipment or laptops, and (3) encryption tools for DMAS data, information and PHI were asked by offerors and discussed.	1) The winning vendor will be required to execute a BAA that will identify all restrictions on DMAS data, information or PHI gathered, used or analyzed during the course of this engagement. The BAA will also address the disposition or destruction of any DMAS data, information or PHI gathered, used or analyzed during the course of this engagement. 2) Restrictions on use of vendor equipment and/or availability of DMAS equipment and encryption tools will be discussed with offerors selected for negotiations. The issues will be settled upon prior to request for best and final offers or award of a contract. 3) DMAS does not anticipate that the winning vendor (contractor) will have any need to use or store any PHI on any equipment.
62.	Questions regarding on-site workspace for vendors were asked by offerors and discussed.	DMAS anticipates making workspace and a workstation available for one or two key staff members during the course of the engagement. This workspace will include phone, facsimile, photo-copy, shredder, Internet/Intranet, and meeting rooms. These resources are available only in connection with the work to be performed (e.g., no long distance personal phone calls, or non-business internet surfing). In response to the requirements of the RFP, in the work plans submitted, offerors are encouraged to identify clearly the work they believe will/can be conducted on-site and offsite. This will be discussed with offerors selected for negotiations, and the issues will be settled prior to request for best and final offers or award of a contract.

Attachment C
RFP 2007-06

Revised Cost Proposal

Services			
Startup Costs			
(Detailed)			
Direct Costs		**Year 1**	**TOTAL**
Labor (by Individual or staff category) *Indicate hourly billing rate for each category*			
Subtotal Labor			
Total Labor			
Travel			
Postage/Delivery			
Telephone/Fax			
Misc (detailed)			
Total Other Direct			
TOTAL			

Note: General and Administrative and other indirect costs must be included in the direct cost figures. (DMAS will not consider G&A or other fees as a separate line item.)

Evaluations of costs will be based on the total Year 1 Cost. Costs of projects that may develop later in Year 1 or in Years 2 & 3 will be based on the negotiated hourly rates submitted for Year 1.